dcstm
Department:
Community Safety and Transport Management
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

2030
NDP

DEPARTMENT OF COMMUNITY SAFETY AND TRANSPORT MANAGEMENT

RISK MANAGEMENT STRATEGY
2025/2026

TABLE OF CONTENTS PAGE

1. GLOSSARY OF TERMS

TERM	DEFINITIONS
Accountability	Refers to the mechanisms for demonstrating how delegated authority has been exercised, and for calling to account those to whom authority has been delegated.
Audit committee	The audit committee's responsibilities include advising on financial and non-financial issues, keeping under review the effectiveness of internal control and risk management systems, and advising the department that satisfactory arrangements are in place to promote economy, efficiency and effectiveness.
Business plan	An output of the strategic planning process, the business plan provides an over-arching strategy for the Departmental strategies.
Collaboration	The processes of two or more people, entities or organisations working together to complete a task or achieve a goal.
Consequence	The outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain.
Cost	The cost of activities, both direct and indirect, involving any negative impact, including money, time labour, disruption, and goodwill, political and intangible losses.
Culture	"Attitudes, behaviours and understanding about risk, both positive and negative, that influence the decisions of management and personnel and reflect the mission, vision and core values of the organization." (COSO)
Department	Department of Community Safety and Transport Management and / or its successor in title.
Departmental Management Committee (DMC)	Refers to all executive and senior management of the Department, including any other official, who the Accounting Officer may appoint or nominate to serve in this committee.

Event	An incident or situation, which occurs in a particular place during a particular interval of time.
Frequency	A measure of the rate of occurrence of an event expressed as the number of occurrences of an event in a given time. See also likelihood and probability.
Governance	The systems and processes that ensure the overall effectiveness of an entity – whether a business, government or multilateral institution
Hazard	A source of potential harm or a situation with a potential to cause loss.
Inherent risk	The risk to the department in the absence of any actions management might take to either alter the risk's likelihood or impact (risk before controls).
Impact	The effect that a risk would have on the Department if it happens.
Likelihood	Used as a qualitative description of probability or frequency.
Loss	Any negative consequence, financial or otherwise.
Monitor	To check, supervise, observe critically, or record the progress of an activity, action or system on a regular basis in order to identify change.
Probability	The likelihood of a specific event, outcome, measured by the ratio of specific events, outcomes to the total number of possible events, or outcomes. Probability is expressed as a number between 1 and 5, with 1 indicating insignificance of an event or outcome and 5 indicating that an event or outcome is certain.
Residual risk	The remaining level of risk after risk treatment measures (controls) have been taken into consideration.
Risk	An unwanted outcome, actual or potential, to the Institution's service delivery and other performance objectives, caused by the presence of risk factor(s). Some risk factor(s) also present upside

	potential, which Management must be aware of and be prepared to exploit. This definition of "risk" also encompasses such opportunities.
Risk acceptance	An informed decision to accept the consequences and the likelihood of a particular risk.
Risk analysis	A systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.
Risk assessment	The overall process of risk analysis and risk evaluation
Risk avoidance	An informed decision not to become involved in a risk situation.
Risk control	Part of risk management, which involves the implementation of policies, standards, procedures and physical changes to eliminate or minimise adverse risks.
Risk culture	Set of shared attitudes, values and practices that characterise how the Department considers its day-to-day activities.
Risk evaluation	The process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria.
Risk financing	The methods applied to fund risk treatment and the financial consequences of risk.
Risk identification	The process of determining what can happen, why and how.
Risk management	A systematic and formalised process to identify, assess, manage and monitor risks.
Risk management process	The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.
Risk management Unit	A business unit responsible for coordinating and supporting the overall Institutional risk management process, but which does not

	assume the responsibilities of Management for identifying, assessing and managing risk.
Risk reduction	is a selective application of appropriate techniques and management principles to reduce either likelihood of an occurrence or its consequences, or both.
Risk register	A database or repository of all the relevant risks to which an entity is exposed.
Risk retention	is an intentionally or unintentionally retaining the responsibility for loss, or financial burden of loss within the organisation
Risk tolerance	The acceptable levels of variation relative to the achievement of objectives.
Risk transfer	The shifting of responsibility or burden for loss to another party through legislation, contract, insurance or other means. Risk transfer can also refer shifting a physical risk or part thereof elsewhere.
Risk treatment	The selection and implementation of appropriate options for dealing with risk.
Six Capital	The six capitals are a more balanced approach to generating holistic and actionable reports and, when integrated into an organisation investment decision-making process, provides sustainable development as behaviour as well as an inspirational set of goals. Six capitals are financial, manufacturing, human, social and relationship, intellectual and natural capital.
Triple context	King IV recommends the use of performance measures that support positive outcomes across the triple context (financial, environmental, and social) in which the organisation operates, and/or all the capitals that the organisation uses or affects.
Stakeholders	People and entities who may affect, be affected by, or perceive themselves to be affected by, a decision or activity.

ABBREVIATIONS	
CGICT	Corporate Governance Information Communication Technology
EXCO	Executive Committee
ICT	Information Communication Technology
PFMA	Public Finance Management Act
RAT	Risk appetite and tolerance level.
PESTLE	Political Economic Social Technological Environment & Legal

2. CONTEXT

Risk Management is recognised as an integral part of responsible management and the Department therefore adopts a comprehensive approach to the management of risk. The Accounting Officer has committed the Department to a process of Risk Management that is aligned to the principles of good corporate governance as anticipated by King IV report and the Public Sector Risk Management Framework.

The Department also has adopted the Public Sector Risk Management Framework, which has been adopted by the Province as a guide to the risk management process. The framework further satisfies the compliance requirements of the Provincial Risk Management Strategic Support Plan approved by **EXCO**.

3. LEGISLATIVE AND OTHER REGULATORY MANDATE

3.1 Public Finance Management Act (Act 1 of 1999 as amended by Act 29 of 1999)

a. Section 38 (1) (a) (i) of the PFMA requires that:

"The accounting officer should have and maintain effective, efficient and transparent systems of financial and risk management and internal control."

b. Section 45 of the Public Finance Management Act (Act 1 of 1999 as amended by Act 29 of 1999) (PFMA).

3.2. Treasury Regulations

a. Paragraph 3.2.1 of Treasury Regulations state that 'the accounting officer must facilitate a risk assessment to determine the material risks to which the institution may be exposed and to evaluate the strategy for managing these risks'.

b. The Accounting Officer must ensure that a risk assessment is conducted at least annually to identify emerging risks of the institution.

c. A risk management strategy, *which must include a fraud prevention plan*, must be used to direct internal audit effort and priority, and to determine the skills required of managers and staff to improve controls and to manage these risks.

d. The strategy must be clearly communicated to all officials to ensure that the risk management strategy is incorporated into the language and culture of the institution.

3.3. CGICT Framework

CGICT Framework involves evaluating and directing the achievement of strategic goals using ICT to enable the departmental business, monitoring of ICT service delivery, and to ensure continuous service improvement. It includes determining strategic goals and plans for ICT service delivery.

Effective Corporate Governance of ICT is achieved in the Department through:

a. Ensuring that business and ICT-related risks do not exceed the Departmental risk appetite and risk tolerance;

b. Ensuring that ICT risks are managed within the Departmental risk management practice.

c. It must also ensure that the ICT function is audited as part of the departmental audit plan.

The Corporate Governance of ICT risks are a continuous function that should be embedded in all operations of a department.

3.4. King IV Report (Principle 11)

a. Provides that" The governing body should govern risk in a way that supports the organization in setting and achieving its strategic objectives"

b. The recommended practices that the governing body should perform, are summarized as:

c. Set the approach for risk governance, including opportunities and risks when developing strategy and the potential positive and negative effects of the same risk on the achievement of objectives.

d. Treat risk as integral part of and adherence to duties, approve risk policy, evaluate and agree the risks it is prepared to take (i.e. risk appetite and risk tolerance levels)

e. Delegate to Management risk management implementation

f. Oversee the risk management (including assessment of risks and opportunities in relation to the triple context and use of 6 capitals, achievement of objectives, dependency on resources as well as the risk responses, business continuity and culture of the organization).

g. Consider receiving periodic, independent assurance on the effectiveness of risk management

h. Disclose nature and extent of risks and opportunities; overview of the risk management system; areas of focus; key risks, unexpected risks, risks taken outside tolerance levels; and actions to monitor and address the risks.

4. RISK MANAGEMENT MISSION STATEMENT

The Department wishes to adopt best practices in the identification, analysis and cost-effective control of risks to ensure that they are reduced to an acceptable level.

It is acknowledged that some risks will always exist and will never be eliminated, however, the Department will continue to utilise available means to control such risks by reviewing current controls regularly. It is imperative that all employees understand the nature of risk and accept responsibility for the risks associated with their area of responsibility. The necessary support, assistance and commitment of senior management will be provided.

The Accounting Officer and Management team has a moral and statutory duty to take all reasonable actions to safeguard its employees, assets, the environment and the public/society; and ensure that the Department is not financially or operationally disrupted. It will meet this mandate by ensuring that risk management plays an integral part in the governance of the Department at a strategic and operational level.

5. OBJECTIVES

The Department requires a comprehensive approach to corporate risk management that promotes broad strategic thinking and analysis, while fundamentally integrating its core values and beliefs. In order to make sure that we fulfil our strategy, our risk management program shall arm management and the other employees with amongst others: -

5.1 A common understanding of risk across multiple functions, directorates and sub directorates,

5.2 Realisation that risk management is everyone's job.

5.3 Proactive identification of risks during the course of duties in a more efficient and cost-effective manner.

5.4 A risk management program that allow people to view the problem from various angles to identify not only the mitigation activities, but also to anticipate and act on potential opportunities,

5.5. Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.

5.6. Build and improve capabilities to respond effectively to low probability and critical risks.

5.7. Achieve cost savings through better management and monitoring of internal resources.

5.8. Provide for the management of risk within the Department with the intention of enhancing service delivery and ensuring improved efficiency and promoting excellence.

5.9. Provide awareness to employees on prevention, detection and reporting of fraud and corruption risk.

5.10. To promote the adoption of e-Government initiative, in the lieu of enabling and supporting the departmental core business activities and other structures within the department.

6. ENTERPRISE RISK MANAGEMENT PROCESS

The risk management process and it benefits are documented fully in the risk management policy. The objective of this strategy took into account the process of risk management;

HK

however, the focus of this strategy will be on how the department respond to those identified risks. The risk responses involve choosing mitigation strategies, which will reduce or eliminate the level of the risk. In responding to the risks identified, one or a combination of the following strategies may be considered: -

6.1 GOVERNANCE AND CULTURE.

The King IV Report on Corporate Governance for South Africa (King IV report), published in 2016, provides one perspective on what defines good governance in the context of ERM-related business and societal changes, such as inequality, climate change, radical transparency and rapid technological and scientific advancements. The King IV report offers a principles-based approach to ethical and effective leadership by the governing body in pursuit of defined outcomes, which include an ethical culture, good performance, effective control and legitimacy. The Department is committed to providing ethical leadership and good governance in laying the foundation of culture that is conducive for all employees and stakeholders. There are five principles for this component.

6.1.1 Exercises Management Risk Oversight

Risk governance and culture start at the top with the influence and oversight of the executive management. Management at executive level are accountable and responsible for risk oversight and possess the required skills, experience and business knowledge.

6.1.2 Establishes Operating Structures

The department executes strategic plan; annual performance plan and/or operational plan and execution of day-to-day operations to achieve its goal and objectives as set out on those plans. Implementation and administration of the abovementioned plans have the potential to introduce new and different risks or complexities.

6.1.3 Defines Desired Culture

COSO frames desired behaviours within the context of culture, core values and attitudes toward risk. The Department is not yet reached a desired level of risk maturity. The department have not assessed the risk culture to check exactly at which level it is standing (risk averse/ risk neutral /risk aggressive). It is imperative that it conduct a survey to verify if officials and management of the department are living up to its core values; also assess the culture and attitude towards risk.

6.1.4 Demonstrates commitment to core values

Culture and tone at the top is defined by the operating style and personal conduct of management must be driven deep down into the department.

6.1.5 Attracts, develops and retains capable individuals

Management have defined the knowledge, skills and experience needed to execute strategy; set appropriate performance targets; attract, develop and retain appropriate personnel and strategic partners; and arrange for succession.

6.2 STRATEGY AND OBJECTIVE-SETTING

Strategy and Objective Setting includes the following principles of the ERM framework:

i. analyse the business context;

ii. define risk appetite;

iii. evaluate alternative strategies and

iv. formulate business objectives.

Strategic Planning, Monitoring and Evaluation directorate within the Department facilitates strategy and Objective Setting process. Management sets strategic objectives, which provide a context for operational, reporting and compliance objectives. The Department do not have a detailed; well-defined risk appetite framework, it is however in the process of developing a detailed risk appetite statement per each objective.

6.3 PERFORMANCE

This component entails processes of identification and assessment risk that may impact the achievement of strategy and business objectives. Risks are prioritized by severity in the context of risk appetite. The Department then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders. Following is a detailed process flow of the components: -

6.3.1 Risk categories

Risks originate from internal sources or from external sources. The table below provides guidance on typical risk categories of institutions, which would also be reflected in its Risk

Universe. Tools such as PESTLE and SWOT analysis are typically used to determine the key internal and external drivers of risk, which could be used to determine and draft the risk categories of an institution.

INTERNAL RISKS	
RISK CATEGORY	**DESCRIPTION**
HUMAN RESOURCE	Risks that relate to human resources of organization. These risks can have an effect on an organization's human capital with regard to: ▪ Integrity & Honesty; ▪ Recruitment; ▪ Skills & competence; ▪ Employee wellness; ▪ Employee relations; ▪ Retention; and ▪ Occupational health & safety.
Knowledge and information management	Risks relating to an organization's management of knowledge and information. The following aspects relate to knowledge and information management: ▪ Availability of information; ▪ Stability of the information; ▪ Reliability and integrity of information data; ▪ Relevance of the information; ▪ Retention; and ▪ Safeguarding of data and information.
Litigation	Risks that the organization might suffer losses due to litigation and lawsuits against it. Losses from litigation can possibly emanate from: ▪ Claims by employees, the public, service providers and other third parties; and ▪ Failure by an organization to exercise certain right that is to its advantage

Loss \ theft of assets	Risks that an organization might suffer losses due to either theft or loss of an asset of the organization.
Material resources (procurement risk)	Risks relating to an organization's material resources. Possible aspects to consider include: ▪ Availability of material; ▪ Costs and means of acquiring \ procuring resources; and ▪ The wastage of material resources.
Information Technology	The risks relating specifically to the organization's IT objectives, infrastructure requirement, etc. Possible considerations could include the following when identifying applicable risks: ▪ Security concerns; ▪ Technology availability (uptime) ▪ Applicability of IT infrastructure; ▪ Integration / interface of the systems; ▪ Effectiveness of technology; and ▪ Obsolescence of technology.
Third party performance	Risks related to an organization's dependence on the performance of a third party. Risk in this regard could be that there is the likelihood that a service provider might not perform according to the service level agreement entered into with an organization. Non-performance could include: ▪ Outright failure to perform ▪ Not rendering the required service in time; ▪ Not rendering the correct service; and ▪ Inadequate / poor quality of performance.
Health & Safety	Risks from occupational health and safety issues e.g. injury on duty; outbreak of disease within the organization.
Disaster recovery and	Risks related to an organization's preparedness or absence

business continuity	thereto to disasters that could impact the normal functioning of the organization e.g. natural disasters, act of terrorism etc. This would lead to the disruption of processes and service delivery and could include the possible disruption of operations at the onset of a crisis to the resumption of critical activities. Factors to consider include: ▪ Disaster management procedures; and ▪ Contingency planning.
Compliance \ Regulatory	Risks related to the compliance requirements that an organization has to meet. Aspects to consider in this regard are: Failure to monitor or enforce compliance; ▪ Monitoring and enforcement mechanisms; ▪ Consequences of non-compliance; and ▪ Fines and penalties paid.
Fraud and corruption	These risks relate to illegal or improper acts by employees resulting in a loss of the organization's assets or resources and irregular expenditure.
Financial	Risks encompassing the entire scope of general financial management. Potential factors to consider include: Cash flow adequacy and management thereof; ▪ Liquidity and solvency; ▪ Financial losses; ▪ Fruitless and wasteful expenditure; ▪ Budget allocations; ▪ Financial statement integrity; ▪ Revenue collection; and ▪ Increasing operational expenditure.

Cultural	Risks relating to an organization's overall culture and control environment. The various factors related to organization culture include: ▪ Communication channels and its effectiveness; ▪ Cultural integration; ▪ Entrenchment of ethics and values; ▪ Goal alignment; and ▪ Management operating style.
Reputation	Factors that could result in the tarnishing of an organization's reputation, public perception and image.

EXTERNAL RISKS	
RISK CATEGORY	**DESCRIPTION**
Economic Environment	Risks related to the organization's economic environment. Factors to consider include: ▪ Credit downgrade; ▪ Inflation; ▪ Foreign exchange fluctuations; and ▪ Interest rates
Political Environment	Risks emanating from political factors and decisions that have an impact on the organization's mandate and operations. Possible factors to consider include: ▪ Political unrest; ▪ Local, Provincial and National elections; and ▪ Changes in key office bearers.
Social environment	Risks related to the organization's social environment. Possible factors to consider include:

	▪ Unemployment; and ▪ Migration of workers.
Natural environment	Risks relating to the organization's natural environment and its impact on normal operations. Consider factors such as: ▪ Depletion of natural resources; ▪ Environmental degradation; ▪ Spillage; and ▪ Pollution.
Technological environment	Risks emanating from the effects of advancements and changes in technology.
Legislative environment	Risks related to the organization's legislative environment e.g. changes in legislation, conflicting legislation.

6.3.1 **Identifies Risk**

The approach to risk identification should be objective/outcome -driven. Risks relating to departmental strategy (strategic plan) are documented on the **strategic risk register**. These risks are associated with the development of the Departmental key strategic outcomes.

There is also the **operational risk register** that is kept for each directorate and/or sub-directorate. The Department is faced in the day-to-day service delivery endeavours with these risks. The risks are documented on the operational register are identified against the outcomes/activities on the operational plan of the Department.

The Department's aim and outcomes have been agreed to and form the basis for medium term strategic plan. Each of the Department's divisions then forged a medium-term plan that outlines the contributions or outcomes of that division to the achievement of the overall Departmental strategic outcomes.

These should drive the critical aspects of the activities – for example, how the Department plan business and allocate resources, how the Department create and revise policies and how performance is measured and reviewed. Clarity of information on key objectives is the first critical component in risk identification; the second is information on relevant threats and opportunities.

Risk Management Unit facilitates identification of risk/threats by individual divisions or programmes within the Department. Risk identification should be viewed as a continuous process rather than an ad-hoc or once-off activity.

The modern view of business risk is encouraged, where risks are viewed as opportunities to be embraced for improvement, not just threats to be avoided.

Each division/programme of the Department shall identify specific risks that impact on its own objectives.

Identification of risks must be supported through proper systems for gathering intelligence. Risk management Unit makes the approach to risk management flexible enough to accommodate new and previously unforeseen risks.

When identifying risks, care should be taken to avoid defining risks with statements, which are simply the converse of the outcomes.

This shall assist the Department to design controls, which are both adequate and effective to address the risk. A statement of the risk should have both the cause and the consequence.

Emerging strategic risks identified during the course of the financial will be presented to Departmental Management Committee to be adopted before presentation to the Risk Management Committee; while the responsible manager/director will approve emerging operational risks.

6.3.2 Assesses and prioritize the risks

The Department like other business have limited resources, so it cannot respond equally to all risks identified across all programmes. Identified risks are therefore assessed based on the likelihood of it occurring and the impact/consequence of its occurrence on the particular outcome/s it is likely to affect. Risk assessment involves rating the inherent risk level and the residual risk level.

The risk index shall be the product of the Likelihood and the Impact, i.e. L X I = RI

a) Likelihood

The probability or frequency of the threat being realised shall be expressed in terms of:

Common (5), Likely (4), Moderate (3), Unlikely (2) and Rare (1) using the definitions below, and in the context of existing controls being in place.

Table 1:

Rating	Assessment	Definition
1	Rare	The risk is conceivable but is only likely to occur in extreme circumstances
2	Unlikely	The risk occurs infrequently and is unlikely to occur within the next 12 months (during the financial year).
3	Moderate	There is an above average chance that the risk shall occur at least once in the next 12 months (during the financial year)
4	Likely	The risk could easily occur, and is likely to occur at least more than once within the next 12 months (during the financial year)
5	Common	The risk is already occurring, or is likely to occur more than once in the next 12 months.

Assigning the best estimate of likelihood can be a simple or a complex question. For example, detailed historical records of flooding can help us to assess the likelihood of future flooding. On the other hand, where little or no previous data exists, it shall be necessary to assign likelihood – for example, that a service provider of an important project shall become bankrupt.

As the Department is trying to predict and describe future events, it should be recognised that there shall be a degree of uncertainties in assessment of risks –, it will involve judgement as well as measurement, and the precise value shall not be known exactly in advance.

b) Impact

The effect of the risk or threat being realised shall be expressed in terms of Critical/catastrophic (5), Major (4), Moderate (3), Minor (2) and Insignificant (1) using the definitions below:

Table 2:

Impact will be **Impact upon**	**Insignificant**	**Minor**	**Moderate**	**Major**	**Critical**
Performance	There is 90-100% that the Outcome will certain be achieved **(Acceptable-No action required).**	There is a 70-89% chance that it is likely that the outcome will be achieved. **(Mostly acceptable-Low level of control intervention required, if any).**	There is 50-69% chances that it is likely that the outcome will be achieved **(Moderate level of control intervention required).**	There is a 30-49% chance that it is likely that the outcome will be achieved. **(Unacceptable level of risk-Major level of control intervention required).**	There is a 1-29% chance that it is likely that the outcome will be achieved. **(Unacceptable-Action must be taken immediately – effective after the approval date of the risk register.)**
Operational Efficiency	Little impact.	Inconvenient delays.	Delays in major deliverables.	Non achievement of major deliverables.	Non-achievement of major/key departmental objectives.
Stakeholder impact	Inconvenience & delays to individuals.	Significant impacts on individuals but no noticeable impact on overall, service delivery.	Major impacts on significant numbers of Individuals, resulting in noticeable impact on overall service delivery.	Major and long term impacts on individuals and overall delivery of services.	Permanent or debilitating/incapacitating impact on individuals and overall delivery of services.
Regulatory/statutory	No noticeable regulatory/statutory impacts.	Minor and temporary non-compliance with regulatory requirements.	Short-term non-compliance with significant regulatory requirements.	Significant non - compliance with essential regulatory requirements	Long-term or indefinite non-compliance with essential regulatory requirements.
Financial Loss	Less than 0.25% of the Operational Budget.	Above 0.25%and less than 0.5% of the Operational Budget.	Above 0.5%and less than 0.75% of the Operational Budget.	Above 0.75% and less than 1% of the Operational Budget.	1% of the Operational Budget and above.
Reputation and image	Unsubstantiated, low impact. Low profile or no news item.	Substantiated, low impact, low news profile.	Substantiated, public embarrassment, moderate impact, moderate news profile.	Substantiated, public embarrassment, high impact, high news. Third party actions	Substantiated, public embarrassment, high multiple impacts, wide spread news profile, third party actions.
Occupational health and safety (injuries)	None	First aid treatment	Medical Treatment required.	Death or extensive injuries.	Multiple deaths or severe permanent injuries.

The more significant the impact (financially, as it affects operations, our reputation and the trading /commercial / regulatory environment, or in raising legal concerns), the higher the potential profile of the risk and the greater its interest to Management.

When assessing the potential financial impact of a risk, we shall consider both the value at risk and the potential cost of rectification, to enable us to manage resources appropriately and focus on those risks with a potentially high impact.

Risks with both common likelihood of occurring and a critical impact shall demand immediate attention of the Accounting Officer and Executive Authority.

Risk assessment allows a Department to consider how potential events might affect the achievement of objectives. Participants assess events by analysing the likelihood and its impact.

The risk assessment shall follow the process outlined below which includes following steps:

c. **Step 1**: The parameters (scoring system / rating) shall be quantified for impact and likelihood before the actual assessment.

The four potential effects of the identified risks are:

i. Impact before controls ***(Inherent Impact -II)***

ii. Likelihood before controls ***(Inherent Likelihood -IL)***

iii. Impact after controls ***(Residual Impact -RI)***

iv. Likelihood after controls ***(Residual Likelihood -RL)***

The identified risks shall be rated (scored) according to the perceived likelihood of occurrence and impact to the Department. This shall be done through the facilitation of meetings or workshops with the participants per their directorate.

d. **Step 2:** The parameters are applied to the risk matrix to indicate what areas of the risk matrix would be regarded as (critical, major, moderate, minor or insignificant).

(Example below refers): -

Table 3

IMPACT	Critical	5	10	15	20	25
	Major	4	8	12	16	20
	Moderate	3	6	9	12	15
	Minor	2	4	6	8	10
	Insignificant	1	2	3	4	5
		Rare	Unlikely	Moderate	Likely	Common
		LIKELIHOOD				

RISK INDEX	RISK MAGNITUDE
20 to 25	CRITICAL
15 to 19	MAJOR
14 to 10	MODERATE
05 to 9	MINOR
1 to 4	INSIGNIFICANT

The green-shaded area represents the area that can be tolerated given the limited resources to mitigate the risks and the nature or source of the risk.

e. **Step 3:** The risk acceptance criterion is also determined by identifying what risks shall not be tolerated: -

Risks with a risk index of greater than 9/nine shall not be tolerated, i.e. all risks with a moderate rating and above as illustrated in the schematic representation below.

Table: Risk acceptability bands/category

RISK MAGNITUDE	RISK - ACCEPTABILITY	ACTIONS PROPOSED
20 - 25	UNACCEPTABLE	Action must be taken immediately, effective from the 0 -3 months.
15 - 19		Action must be taken immediately, effective from 0 – 3 months.
10- 14		Action must be taken immediately, 0 - 6 months.
5 - 9	ACCEPTABLE	Limited or low intervention, control and monitor, report to Management.
1 – 4		

NB: Implementation period means that implementation of action(s) has commenced or in progress as opposed to full implementation.

6.3.3. Implements Risk Responses

The risk responses involve choosing mitigation strategies, which will reduce or eliminate the level of the risk. In responding to the risks identified, the following strategies may be considered: -

a. **Risk Treatment**, also known as risk mitigation or minimisation – by far the greater number of risks will be in this category. The purpose of treatment is not necessary to terminate the risk but, more likely, to set in train a planned series of mitigation actions to contain the risk to an acceptable level; and

b. **Risk Transfer,** this might be done through such things as conventional insurance or by asking a third party to take on the risk in another way. Outsourcing some of our services, for example, transfers some, but not all, of our risks (and often introduces a new set of risks to be managed);

c. **Risk Tolerance**, our ability to take effective action against some risks may be limited, or the cost of taking action may be disproportionate to the potential benefit gained – cost benefit analysis. In this instance, the only management action required is to 'watch' the risk to ensure that its likelihood and impact does not change. If new management options arise, it may become appropriate to treat this risk in the future;

d. **Risk Termination** - this is a variation of the 'treat' approach, and involves quick and decisive action to eliminate a risk altogether. The introduction of new technology may also remove certain existing risks, though it will often result in a new set of risks to be addressed.

e. **Risk Avoidance -** not engaging in the activity that creates risk exposure,

f. **Risk Exploitation** - it is an option that should be considered whenever tolerating, transferring or treating a risk. There are two aspects to this. The first is whether or not at the same time as mitigating threats; an opportunity arises to exploit positive impact. The second is whether circumstances arise which, whilst not generating threats, offer positive opportunities. For example, a drop in the cost of goods or services frees up resources, which can be re-deployed to other service delivery imperatives.

g. **Integrating** some or all - applying some or all of the risk response to address a risk.

6.3.4. Develops Portfolio View

This is the stage in the process where Management has taken a decision to treat the risk. Those choices will be recorded on the risk registers. Existing control activities are viewed as critical steps to mitigating the risks, additional to that risk treatment plans will be required to augment or close the gaps that could be remaining after implementation control activities. Control Activities refers various measures implemented to mitigate or ensure that risks are minimised to an acceptable level. Policies and procedures applied by Management through various processes in the Department are examples of control activities. The option of "treat" in addressing risk can be further analysed into four different types of controls:

a. **Preventive Controls** - These controls are designed to limit the possibility of an undesirable outcome being realised. Examples of preventive controls include separation of duty, whereby no one person has authority to act without the consent of another (such as the person who authorises payment of an invoice being separate from the person who ordered goods prevents one person securing goods at public expense for their own benefit),

b. **Corrective Controls -** They provide a route of recourse to achieve some recovery against loss or damage. An example of this would be design of contract terms to allow recovery of overpayment.

c. **Directive Controls** - These controls are designed to ensure that a particular outcome is achieved. They are particularly important when it is critical that an undesirable event is avoided - typically associated with Health and Safety or with security. Examples of this type of control would be to include a requirement that protective clothing be worn during the performance of dangerous duties, or that staff be trained with required skills before being allowed to work unsupervised.

d. **Detective Controls** - These controls are designed to identify occasions of undesirable outcomes having been realised. Their effect is, by definition, "after the event" so they are only appropriate when it is possible to accept the loss or damage incurred. Examples of detective controls include stock or asset checks (which detect whether stocks or assets have been removed without authorisation), reconciliation (which can detect unauthorised transactions), "Post Implementation Reviews" which detect lessons to be learnt from projects for application in future work, and monitoring activities which detect changes that should be responded to.

7. REVIEW & REVISION

The fourth component focuses on monitoring risk management performance. Effective monitoring provides insight into the relationship between risk and performance, how strategic risks are affecting performance, and emerging risks. There are three principles for this component;

- Assesses Substantial Change
- Reviews Risk and Performance
- Pursues Improvement in ERM

7.1 Assesses Substantial Change

Continuous monitoring of substantial changes in the internal or external environment is very important; that would enable the department to determine if there are any shifts that could trigger a change on the risk profile and require a response or decision from Management.

The changes would probably give rise to a new risk/s, or exacerbate or lessen the potential impact of an existing risk, risk management should consider if action is warranted – such as a change to the risk register, a new risk assessment or investment in a risk response.

7.2 Reviews Risk and Performance

Monitoring, is implemented to help ensure "that internal control continues to operate effectively as initially intended; and that is one of the fundamental components of the risk management process. It is of ensuring that internal controls continue to operate effectively as initially intended.

Ongoing monitoring is undertaken by Management at process level so that set targets/objectives are met and if not, corrective measures are made timeously; while separate evaluation could be provided by a number of parties inside or outside of the Department.

7.3 Pursues Improvement in ERM

ERM should be improved continuously over time. Even mature ERM processes can become more efficient and effective in increasing its value contribution.

Risk management team, Internal Audit team, and AGSA and Regulatory structures like Office of the Premier, Provincial Treasury, and Provincial Legislature etc.; undertake continuous and separate evaluations of internal control systems. The purpose of these evaluations is to identify areas of improvements. A collective monitoring process of this nature is called Combined Assurance. Detailed information relative to this is documented in the departmental Combined Assurance Policy Framework.

Subsequent to both internal and external audits, risk management unit through Internal Control sub-unit make follow-ups on the queries/findings raised by auditors, to ensure that the recommendations made are being implemented and hence no future re-occurrence.

Risk management team conduct the risk monitoring process on monthly basis and consolidate the reports for quarterly reporting. This is done in order to verify whether there is any progress registered in management of risks or not, also to make necessary changes to the risk registers (risk definition, causes, consequences, risk ratings, current controls, treatment plans and its implementation dates).

Quarterly risk monitoring together with verifying the relevant portfolio of evidence related to progress reported, and that is documented on the risks monitoring tool developed. The risk owner and/or risk coordinator, risk management practitioner sign the monitoring tool each time quarterly monitoring is conducted.

8. INFORMATION, COMMUNICATION & REPORTING

The final component recognises the vital need for a continuous process to obtain and share relevant information. This information for decision-making must flow up, down and across the Department and provide insight to key stakeholders. There are three principles for this component: -

8.1 Leverages Information and Technology

Departmental Information contained in ICT resources shall be accessed or communicated / handled in a manner that is compliant to the ICT Security Policy prescripts.

8.2 Communicates Risk Information

Relevant information should be properly and timeously communicated to allow relevant officials to identify, assess and respond to risks. Officials within programmes should be in a position to identify risks and report such to their managers.

8.3. Reports on Risk, Culture and Performance

The primary objective of communication and reporting is to provide decision-useful information on risk management approach and performance. It is important to communicate how well the risks are being managed and provide information to support better decision-making processes across the Department.

Quarterly progress reports from programme and sub programme managers should be submitted to the risk management unit to enable them to consolidate into a quarterly risk monitoring report. The report is then presented to Extended Departmental Management Committee (EDMC) meeting where quarterly performance of the Department is reviewed; the report is also presented at the Risk Management Committee and Audit Committee. Risk reporting also provides awareness of risks across the Department.

9. RISK REGISTER

To manage risk properly, appropriate documentation is required. The Risk Management Unit facilitates the process of risk identification and provide guidance for documenting the results of the process. All levels of officials within the Department will be involved in this process.

The identified risks, once assessed in terms of likelihood of occurrence and impact, they are recorded on the risk register. The Department keeps the strategic or key risk register and the operational risk register. Strategic risks emanate from the strategic objectives made by the department. The process to identify such risks is integrated to the annual strategic planning process of the Department. The strategic risk register is recommended for approval by the Chairperson of the Risk Management Committee (RMC) and approved by the Head of the Department.

The main contents or details of the register are as follows: -

a. The Strategic outcome

b. The Risk description

c. The cause of the risk

d. The consequence of the risk

e. Inherent impact and likelihood

f. Current control

g. Residual impact and likelihood

h. Risk response option

i. Treatment plans/Mitigation strategies

j. Risk owner

k. Action owner

l. Start and end date of implementing the treatment plan.

m. The progress made on the agreed treatment plans

10.MONITORING IMPLEMENTATION OF RISK TREATMENT PLANS

10.1 Monitoring and Reporting.

a. Requests of risk monitoring reports

Risk Management request progress reports from Management monthly, progress reports requested relates to the implementation of the risk treatment plans for both strategic and operational risks. Risk Management Unit will analyses the reported progress, which should be supported by relevant portfolio of evidence, and thereafter compile the risk monitoring report based on the outcomes of the reported information.

b. Analysis of progress reports.

In implementation of treatment plans, there are progressive stages/rankings used to measure or classify the implementation status, namely; -

i. **Completed** – the risk treatment plan has been implemented fully,

ii. **In progress –** the process to implement has started and ongoing

iii. **Not yet started** – the treatment plan's date of implementation is still in the future

iv. **Overdue** – the date of implementation has passed.

v. **Deferred** – request to move the implementation to the future date (based on the reasons provided)

vi. **Progress not submitted** – refers to a situation where Management for some reasons did not submit progress reports. It is meant to attract the attention and intervention of Management; therefore, status should not be carried to the final reports.

c. Risk reports

Monitoring is conducted monthly, and reports are consolidated into quarterly risk monitoring reports, which should be presented at the Departmental Management Committee first i.e. either EDMC, DMC or EMC; thereafter to the Risk Management Committee.

11. RISK APPETITE AND TOLERANCE FRAMEWORK

Risk appetite (RAT) framework captures the Departmental viewpoint for taking and managing risks, also helps to structure the Department's expected risk culture and most importantly guides overall resource allocation. While the risk tolerance identifies the specific minimum and maximum levels, beyond which the Department is unwilling to lose due to decisions on certain activities. It is expressed in quantitative terms that can be monitored; it is often communicated in terms of acceptable or unacceptable outcomes or as limited levels of risk. Risk appetite is more culture forming whereas risk tolerance is where you will often find Key Risk Indicators (KRIs) to set boundaries. Table 3. (Page 24) indicates the tolerable or acceptable level risk the Department has set.

The Department faces a broad range of risks, which are reflective of its goals and objectives as outlined in the Medium Term Strategic Framework. Risks identified cover amongst others; the environment in which the Department is operating to execute its mandate; financial operations, the socio-economic issues, as well as its day-to-day operational activities.

11.1 Over-arching Risk Appetite statement

The Department employs limited resources available to mitigate high priority or high-risk areas in order to reduce such risks to an acceptable level. It cannot also, ostensibly assume a high level of risk appetite that would render risk around safety of communities unmanaged. In this regard, strategic outcomes of the Department can best be achieved if the Department lowers, quite significantly its Risk Appetite.

Department strives to maintain a low appetite for risk; however, it is acknowledging that in pursuit of the mandate at times activities that inherently carry greater risks may be undertaken. Where the Department chooses to accept an increased level of risk it will do so, subject always to ensuring that the potential benefits and threats are fully understood before actions are authorised, that it has sufficient risk capacity, and that sensible and proportionate measures to mitigate risk are established.

And as a result, the risk appetite will often be different at an activity level compared to enterprise-wide level, hence a need for a detailed risk appetite and tolerance framework for the Department. The exercise to develop a detailed risk appetite and tolerance framework will be finalised during the current financial year.

12. DEVELOPING THE STRATEGY

Development of this strategy has taken into account the Committee of Sponsoring Organisations (COSO) model and Public sector risk management framework (EWRM). The strategy consequently views risk management in relation to (business) objective setting, risk identification, risk assessment, risk response and control, communication and monitoring. This document should to be read/used in conjunction with the other Departmental policies, e.g.

a. Risk management policy
b. Risk appetite and tolerance framework
c. Risk management Committee charter
d. Anti-Corruption, Ethics and Integrity Plan
e. Anti-Corruption, Ethics and Integrity Policy
f. Departmental Strategic Plan for Information Technology
g. Business Continuity Management Policy
h. Security policy
i. OHS policy, etc.

13. FRAUD PREVENTION PLAN

The Treasury Regulations requires the accounting officer to ensure that a risk assessment is conducted at least annually to identify emerging risks of the institution.

A risk management strategy, ***which must include a fraud prevention plan***, must be used to direct internal audit effort and priority, and to determine the skills required of managers and staff to improve controls and to manage these risks.

The Department has developed and implemented the **Anti-corruption, ethics and integrity management policy** in order to mitigate the fraud related risks, which might impact on the Department. The plan recognises 4 main components in its fight against fraud and corruption, namely: ***Prevention, Detection, Investigation and Resolution*** of fraud and corruption cases.

Fraud risk assessment is the first line defence mechanism, a measure that the Department undertakes in order to deal proactively with acts of fraud and corruption threatening the Department.

A whistle blowing policy, which outlines procedures to be followed in disclosing acts of fraud, corruption and/or other concerns, and how whistle blowers will be protected, is also developed.

14. BUSINESS CONTINUITY AND RECOVERY PLANS

Business Continuity and Recovery Plans are the most critical strategies of mitigating risks of low probability of occurrences and high impact risks, e.g. Natural or man-made disasters and business interruptions or shutdowns.

The Department shall also adopt an integrated and comprehensive approach to risk management through business continuity planning and recovery plans. This shall however be a separate document to this policy and shall highlight plans and measures by different units on how they shall continue delivering services during disasters and their recovery processes.

The Business Impact Analysis (BIA) undertaken for critical business processes within the Department will inform the Business Continuity plan. The Department has developed a policy and guidelines to guide the development of the Business Continuity Plan.

15. COMBINED ASSURANCE POLICY FRAMEWORK

Combined assurance process is defined as "a holistic and strategic focused assurance model, that integrates assurance activities based on the business model and risk profile, matched with the effectiveness of systems, controls and reporting structures to preserve, protect and grow institution value, whilst minimising risk exposure and optimising opportunities and returns for best long term interest of the organisation, its shareholders and stakeholders and performance and results based" King IV. It is also a planned approach to assess the extent and adequacy of assurance coverage on key departmental risks and reporting thereon to Senior Management, the Risk Management Committee, Audit Committee and other regulatory bodies.

The Department has adopted a five line of assurance approach as per guidance of King IV report. Risk Management function plays the lead role in combined assurance, there are key dimensions that should be carefully managed, such as; *A combined assurance plan*; *appropriate assurance activities and standards*; *competent assurance service providers*; the *combined assurance process and report*.

16. RISK MANAGEMENT COMMITTEE

The Risk Management Committee will be appointed as per the charter or terms of reference and will discuss the progress as presented by the Risk Management Unit regarding risk management processes and recommend improvement where necessary. Amongst others, the Committee will discuss the following reports:

a. Progress reports on implementation of risk mitigation strategies
b. OHS reports
c. Loss control reports
d. Progress on implementation of the procurement plan
e. Expenditure report
f. Quarterly Performance reports (PI) and validation reports
g. Progress on reported cases of fraud and corruption

17. EVALUATION OF RISK MANAGEMENT EFFECTIVENESS

Evaluation of risk management effectiveness is vital to maximise the value created through risk management practices. The Department should strive to incrementally and sustainably achieve a mature risk management regime in order to realise positive outcomes due to implementation of risk management processes.

The Department will utilise the following ***performance indicators to measure the value add of its risk management processes***:

a. Periodically measuring outcomes against pre-set key performance indicators aligned to the overall goals and objectives through quarterly performance review sessions, including comparison of year-on year performance.

b. Utilise the Risk Management Maturity Capability Model from Provincial Risk Management Unit to evaluate the current and progressive risk management maturity.

c. Percentage change in unauthorised, irregular, fruitless and wasteful expenditure based on year-on year comparisons.

d. Percentage change in incidents and quantum of fraud and corruption based on year-on-year comparisons.

e. Progress in securing improved audit outcomes in regularity and performance based on year-on-year comparisons.

f. The Department's collective awareness, skill and participation in risk management.

g. Implementation of risk management and audit action plans.

h. Co-operation between the Risk Management Unit, Risk Management Committee, Risk Champion and relevant stakeholders involved in risk management.

i. Quality and timeliness of risk identification, assessment and reporting.

j. Proactive identification of new and emerging risks and absence of surprises.

18. MONITORING EFFECTIVENESS OF THE STRATEGY

As required for any strategy to be evaluated, the risk management strategy will be assessed to determine its effectiveness and adequacy in mitigating departmental risks. There are instruments available to the Department to measure the effectiveness of its risk management strategy.

a. Analysis of the divisional quarterly risk reports and the key performance indicators reflected thereon.

b. Assurances provided by the Provincial Internal Audit, Auditor General and Provincial Treasury.

c. Monitoring and reporting on the Integrated Risk Management Implementation Plan to the strategy. ***Attached as Annexure B.***

d. Complete the risk maturity tool provided by the Provincial Risk Management Support and return it for analysis.

19. CONCLUSION

The Department believes that risk management makes good business sense and it is an essential tool in the environment in which it operates.

It is understood that risk management is not an end in itself, but rather an important means towards achievements of goals and objectives. It cannot and does not operate in isolation, but rather is an enabler of the management process. Risk Management is interrelated with corporate governance by providing information to Departmental Management Committee on the most significant risks and how they are being managed.

20. REVIEW OF THE STRATEGY

The Accounting Officer shall review this strategy annually to incorporate any changes that may occur in the Department and be implemented effective from the date of approval.

21. RECOMMENDATION AND APPROVAL

DISCUSSED AND ADOPTED DURING	DATE
DEPARTMENTAL MANAGEMNT COMMITTEE	26 /03/2025
RISK MANAGEMENT COMMITTEE	26 /03/2025

RECOMMENDED

MR. A KYEREH

CHAIRPERSON

DATE: 27/03/2025

APPROVED BY:

DR. H. KEKANA

HEAD OF DEPARTMENT

DATE: 31/03/2025

ANNEXURES

ANNEXURE A – RISK MANAGEMENT IMPLEMENTATION PLAN

ANNEXURE B – DEPARTMENTAL RISK REGISTER

ANNEXURE C – RISK MONITORING TOOL